

.....
(Original Signature of Member)

118TH CONGRESS
1ST SESSION

H. R. _____

To direct the Director of the Cybersecurity and Infrastructure Security Agency to establish a School Cybersecurity Improvement Program, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Ms. MATSUI introduced the following bill; which was referred to the Committee on _____

A BILL

To direct the Director of the Cybersecurity and Infrastructure Security Agency to establish a School Cybersecurity Improvement Program, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may cited as the “Enhancing K–12 Cyberse-
5 curity Act”.

1 **SEC. 2. SCHOOL CYBERSECURITY INFORMATION EX-**
2 **CHANGE.**

3 (a) ESTABLISHMENT.—The Director of the Cyberse-
4 curity and Infrastructure Security Agency shall enhance
5 existing information exchange efforts implemented
6 through partnerships with one or more information shar-
7 ing and analysis organizations to focus specific attention
8 on the needs of K–12 organizations with regard to cyber-
9 security, including a new publicly accessible website (to be
10 known as the “School Cybersecurity Information Ex-
11 change”) to disseminate information, cybersecurity best
12 practices, training, and lessons learned tailored to the spe-
13 cific needs, technical expertise, and resources available to
14 K–12 organizations in accordance with subsection (b).

15 (b) DUTIES.—In establishing the School Cybersecu-
16 rity Information Exchange under subsection (a), the Di-
17 rector shall—

18 (1) engage appropriate Federal, State, local,
19 and nongovernmental organizations to identify, pro-
20 mote, and disseminate information and best prac-
21 tices for local educational agencies, state educational
22 agencies, and educational service agencies (as such
23 terms are defined in section 8101 of the Elementary
24 and Secondary Education Act of 1965 (20 U.S.C.
25 7801)) with respect to cybersecurity, data protec-

1 tion, remote learning security, and student online
2 privacy;

3 (2) maintain a database for an elementary
4 school, secondary school, local educational agency,
5 State educational agency, and educational service
6 agency to identify cybersecurity security tools and
7 services funded by the Federal Government, as well
8 as tools and services recommended for purchase with
9 State and local government funding; and

10 (3) provide a searchable database for an ele-
11 mentary school, secondary school, local educational
12 agency, State educational agency, and educational
13 service agency to find and apply for funding oppor-
14 tunities to improve cybersecurity.

15 (c) CONSULTATION.—In carrying out the duties
16 under subsection (b), the Director shall consult with the
17 following:

18 (1) The Secretary of Education.

19 (2) The Director of the National Institute of
20 Standards and Technology.

21 (3) The Federal Communication Commission.

22 (4) The Director of the National Science Foun-
23 dation.

24 (5) The Federal Bureau of Investigation.

1 (6) State and local leaders, including, when ap-
2 propriate, Governors, employees of State government
3 departments and agencies, members of State legisla-
4 tures and State boards of education, local edu-
5 cational agencies, State educational agencies, rep-
6 resentatives of Indian tribes, teachers, principals,
7 other school leaders, charter school leaders, special-
8 ized instructional support personnel, paraprofes-
9 sionals, administrators, other staff, and parents.

10 (7) When determined appropriate by the Direc-
11 tor, subject-matter experts and expert organizations,
12 including nongovernmental organizations, vendors of
13 school information technology products and services,
14 cybersecurity insurance companies, and cybersecu-
15 rity threat companies.

16 **SEC. 3. CYBERSECURITY INCIDENT REGISTRY.**

17 (a) IN GENERAL.—The Director of the Cybersecurity
18 and Infrastructure Security Agency shall establish,
19 through partnerships with one or more information shar-
20 ing and analysis organizations, a voluntary registry of in-
21 formation relating to cyber incidents affecting information
22 technology systems owned or managed by a covered entity,
23 and determine the scope of cyber incidents to be included
24 in the registry and processes by which incidents can be
25 reported for collection in the registry.

1 (b) USE.—Information in the registry established
2 pursuant to subsection (a) may be used to—

3 (1) improve data collection and coordination ac-
4 tivities related to the nationwide monitoring of the
5 incidence and impact of cyber incidents affecting a
6 covered entity;

7 (2) conduct analyses regarding trends in cyber
8 incidents against such entity;

9 (3) develop systematic approaches to assist such
10 entity in preventing and responding to cyber inci-
11 dents;

12 (4) increase the awareness and preparedness of
13 a covered entity regarding the cybersecurity of such
14 covered entity; and

15 (5) identify, prevent, or investigate cyber inci-
16 dents targeting a covered entity.

17 (c) INFORMATION COLLECTION.—The Director of the
18 Cybersecurity and Infrastructure Security Agency may
19 collect information relating to cyber incidents to store in
20 the registry established pursuant to subsection (a). Such
21 information may be submitted by a covered entity and may
22 include the following:

23 (1) The dates of each cyber incident, including
24 the dates on which each such incident was initially
25 detected and the dates on which each such incident

1 was first publicly reported or disclosed to another
2 entity.

3 (2) A description of each cyber incident, which
4 shall include whether each such incident was as a re-
5 sult of a breach, malware, distributed denial of serv-
6 ice attack, or other method designed to cause a vul-
7 nerability.

8 (3) The effects of each cyber incident, including
9 descriptions of the type and size of each such inci-
10 dent.

11 (4) Other information determined relevant by
12 the Director.

13 (d) REPORT.—The Director of the Cybersecurity and
14 Infrastructure Security Agency shall make available on
15 the School Cybersecurity Information Exchange estab-
16 lished under section 2 an annual report relating to cyber
17 incidents affecting elementary schools and secondary
18 schools which includes data, and the analysis of such data,
19 in a manner that—

20 (1) is—

21 (A) de-identified; and

22 (B) presented in the aggregate; and

23 (2) at a minimum, protects personal privacy to
24 the extent required by applicable Federal and State
25 privacy laws.

1 (e) COVERED ENTITY DEFINED.—In this section, the
2 term “covered entity” means the following:

- 3 (1) An elementary school.
- 4 (2) A secondary school.
- 5 (3) A local educational agency.
- 6 (4) A State educational agency.
- 7 (5) An educational service agency.

8 **SEC. 4. K–12 CYBERSECURITY TECHNOLOGY IMPROVEMENT**
9 **PROGRAM.**

10 (a) ESTABLISHMENT.—The Director of the Cyberse-
11 curity and Infrastructure Security Agency, shall establish,
12 through partnerships with one or more information shar-
13 ing and analysis organizations, a program (to be known
14 as the “K–12 Cybersecurity Technology Improvement pro-
15 gram”) to deploy cybersecurity capabilities to address cy-
16 bersecurity risks and threats to information systems of el-
17 ementary schools and secondary schools through—

- 18 (1) developing cybersecurity strategies and in-
19 stallation of effective cybersecurity tools tailored for
20 K–12 schools;
- 21 (2) making available cybersecurity services that
22 enhance the ability of K–12 schools to protect them-
23 selves from ransomware and other cybersecurity
24 threats; and

1 (3) continuing training opportunities on cyber-
2 security threats, best practices, and relevant tech-
3 nologies for K–12 schools.

4 (b) REPORT.—The Director of the Cybersecurity and
5 Infrastructure Security Agency shall make available on
6 the School Cybersecurity Information Exchange estab-
7 lished under section 2 an annual report relating to the
8 impact of the K–12 Cybersecurity Technology Improve-
9 ment Program, including information on the cybersecurity
10 capabilities made available to information technology sys-
11 tems owned or managed by elementary schools, secondary
12 schools, local educational agencies, State educational
13 agencies, and educational service agencies, the number of
14 students served, and cybersecurity incidents identified or
15 prevented.

16 **SEC. 5. AUTHORIZATION OF APPROPRIATIONS.**

17 There are authorized to be appropriated to carry out
18 this Act \$10,000,000 for each of fiscal years 2024 and
19 2025.

20 **SEC. 6. DEFINITIONS.**

21 In this Act:

22 (1) EDUCATIONAL SERVICE AGENCY.—The
23 term “educational service agency” has the meaning
24 given that term in section 8101 of the Elementary

1 and Secondary Education Act of 1965 (20 U.S.C.
2 7801).

3 (2) ELEMENTARY SCHOOL.—The term “elemen-
4 tary school” has the meaning given that term in sec-
5 tion 8101 of the Elementary and Secondary Edu-
6 cation Act of 1965 (20 U.S.C. 7801).

7 (3) INFORMATION SHARING AND ANALYSIS OR-
8 GANIZATION.—The term “information sharing and
9 analysis organization” has the meaning given that
10 term in section 2200 of the Homeland Security Act
11 of 2002 (6 U.S.C. 650).

12 (4) LOCAL EDUCATIONAL AGENCY.—The term
13 “local educational agency” has the meaning given
14 that term in section 8101 of the Elementary and
15 Secondary Education Act of 1965 (20 U.S.C. 7801).

16 (5) STATE EDUCATIONAL AGENCY.—The term
17 “State educational agency” has the meaning given
18 that term in section 8101 of the Elementary and
19 Secondary Education Act of 1965 (20 U.S.C. 7801).

20 (6) SECONDARY SCHOOL.—The term “sec-
21 ondary school” has the meaning given that term in
22 section 8101 of the Elementary and Secondary Edu-
23 cation Act of 1965 (20 U.S.C. 7801).